Oriental Journal of Computer Science & Technology Vol. **3**(1), 121-124 (2010)

VPN and IPSEC server with IDS

ANIL RAJPUT[1], MANMOHAN SINGH[2], NAVEEN KHER[3]*, SHUMALI KANKANE[4] and PAWAN MEENA[5]

[1]Department of Maths & Computer Science, Sadhuvasvani College, Bhopal, (India).
[2]Department of Computer Science & Engineering, BIST, Bhopal (India).
[3]Saifia College, Bhopal (India). [4]NIIST, Bhopal (India), [5]PCST, Bhopal (India).

(Received: May 12, 2010; Accepted: June 03, 2010)

ABSTRACT

Virtual Private Networking, or VPN, is a technology that lets people access their office's computer network over the Internet while at home or traveling. Accessing a network in this way is referred to as remote access. (For comparison, another common form of remote access is dialing in to the office network over a telephone line.) But VPN is useful for more than just remote access. It can also be used to link two separate offices over a distance. This is sometimes called a "persistent VPN tunnel", or "site-to-site VPN".

Keywords: Virtual Private Networking, & IPSEC Server, IDS.

INTRODUCTION

A **virtual private network** (**VPN**) links 2 computers through an underlying local or wide-area network, while encapsulating the data and keeping it private. Imagine a pipe within a pipe, and you will have the concept. Even though the outer pipe contains the Before encapsulation,the packets are encrypted so the data is unreadable to outsiders.Packets are separated and returned to their original format.

IPSec

Internet Protocol security (IPsec) is a framework of open standards for protecting communications over Internet Protocol (IP) through the use of cryptographic security supports network-level peer authentication, data origin authentication, data integrity& data confidentiality. Inner one, the inner pipe has a wall that blocks the other traffic in larger outer pipe. To the rest of the network, **Virtual Private Networking** technology provides the medium to use the public Internet backbone as an appropriate channel for private data communication. With **encryption and encapsulation technology**, a VPN essentially carves out a private passageway through the Internet and allow remote offices, company road warriors, and even business partners or customers to use the Internet, rather than pricey private lines, to reach company networks. Tunneling is a way to transfer data between two similar networks over an intermediate network. Also called **"encapsulation,"** tunneling encloses one type of data packet into the packenother protocol.

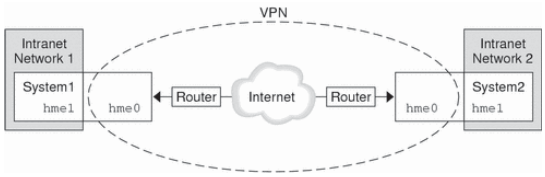
Internet Protocol Security (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways .

IDS

An **IDS** is a device (or application) that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.

Virtual Private Networks

You can use IPsec to construct a virtual private network (VPN). You use IPsec by constructing an Intranet that uses the Internet infrastructure. For example, an organization that uses VPN technology to connect offices with separate networks, can deploy IPsec to secure traffic between the two offices The following figure illustrates how two offices use the Internet to form their VPN with IPsec deployed on their network systems.

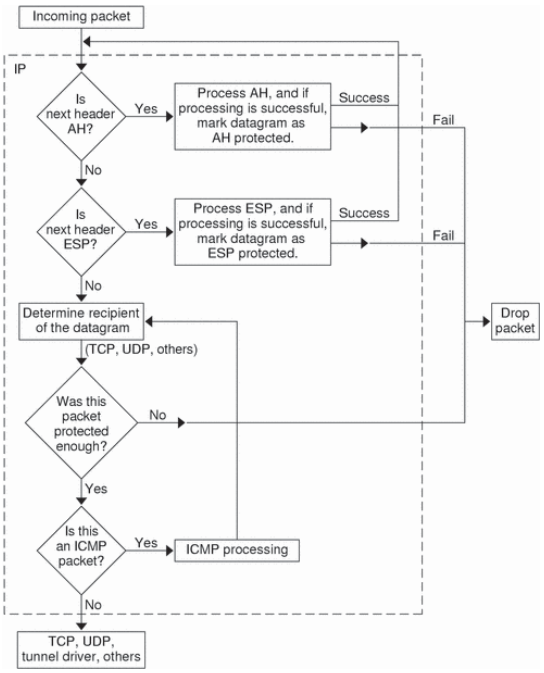


Virtual Private Network

VPN CLASSIFICATION

VPN technologies have myriad protocols, terminologies and marketing influences that define them. For example, VPN technologies can differ:

- In the protocols they use to tunnel the traffic
- In the tunnel's termination point, the customer edge or network provider edg
- In whether they offer site-to-site or remote access connectivity



IDS TERMINOLOGY

- **True Positive**- A legitimate attack which triggers an IDS to produce an alarm .
- **True Negative**- When no attack has taken place and no alarm is raised..
- **Site policy**- Guidelines within an organization that control the rules and configurations of an IDS .
- **Site policy awareness**- The ability an IDS has to dynamically change its rules and configurations in response to changing environmental activity.
- **Confidence value**- A value an organization places on an IDS based on past performance and analysis to help determine its ability to effectively identify an attack .
- **Alarm filtering**- The process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks.

Limitations

- **Noise** - Noise can severely limit an Intrusion detection systems effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate [3].
- **Too few attacks**- It is not uncommon for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored [3].
- **Signature updates** - Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to new strategies.

At the Client Side

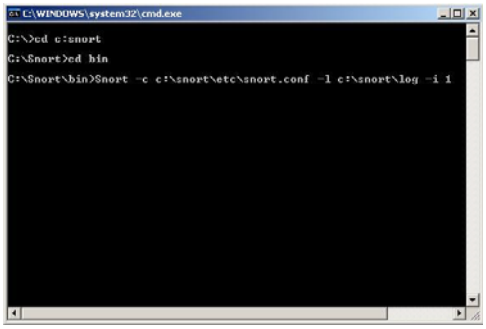
- Step1:
- Go to MY NETWORK PLACES – VIEW NETWORK CONNECTION – ADD NEW NETWORK – VPN ACCESS.
- Step2:
- Give the name of VPN & also the IP ADDRESS of the server & finish.
- Step3:
- Than connect to VPN by giving username of server account (administrator) & password.

Configuring IPSec:

- You configure IPSec through configuring the following aspects of IPSec policies: Assign the predefined default IPSec policies. Creating customized IPSec policies that includes customized rules and filters. Control how IPSec policies are applied. Apply IPSec policies at different levels on the network. You can use either of these methods to configure IPSec policies: You can use the IP Security Policy Management snap-in to configure IP security policies on the local computer. To create a new IPSec policy, you have to right-click the IP Security Policies node in the IP Security Policy Management snap-in, and then click Create IP Security Policy.
- You can use the Group Policy Object Editor snap-in to change local and domain GPOs. To create a new IPSec policy, you have to right-click the IP Security Policies node in the Group Policy Object Editor and then click Create IP Security Policy. When you open the Security Policy Management snap-in, the following predefined default IPSec policies are displayed:
- **Client (Respond Only):** The Client (Respond Only) default IPSec policy has the following characteristics: Least secure default policy. The computer assigned the policy never initiates secure data communication. The computer only responds to IPSec requests from other computers who request it. Contains the default response rule that creates dynamic IPSec filters for inbound and outbound traffic based on the protocol and port which was requested. The predefined policy settings for the Client (Respond Only) default IPSec policy are listed here: IP Filter List; All Filter Action; None Authentication. Kerbero Tunnel Setting; **Secure Server (Request Security):** The Secure Server (Request Security) default IPSec policy has the following characteristics: The computer prefers and initiates secure data communication. If the other computer supports IPSec, secure data communication will take place If the other computer does not support IPSec, the computer will allow unsecured communication with that computer.
- The predefined policy **Secure Server (Require Security):** The Secure Server (Require Security) default IPSec policy has the following characteristics: Only secure data communication is allowed. If the other computer does not support IPSec, the connection is not established Contains three rules, and predefined policy settings: The predefined policy settings for Rule 1 are IP Filter List; All IP Traffic Filter Action; Require Security The predefined policy settings for Rule 2 are: IP Filter List; All ICMP Traffic Filter Action; Permit Authentication; Kerberos Tunnel Setting; None Connection Type; Al The predefined policy settings for Rule 3 are: IP Filter List; Dynamic Filter Action; Default Response Authentication; Kerbero Tunnel Setting; None Connection Type; All You can also create customized IPSec policies that

include customized rules and filters that suit specific security requirements of the organization. Customized IPSec policies can be created in the IP Security Policy Management MMC. You can also create your own IPSec policy by using the IP Security Wizard which you can initiate from within the IP Security Policy Management MMC.

- **The Properties dialog box of an IPSec policy contains the following tabs:**
- **General tab** used to configure general type configuration settings for he IPSec policy, including the following: Configure the policy name in the Name text box. Specify a description for the policy in the Description text box. Specify the interval for which clients using this specific policy checks for policy updates in the Check For Policy Changes Every box. Set the key exchange settings for the policy by clicking.



CONCLUSION

The system developed is very flexible and new enhancements can be added to it to increase functionality and efficiency of this project titled "**VPN & IPSec Server with IDS".** Configured on Window Server 2003 and IDS configured by Snort_2_8_5_3 & WinPcap_4_1_1 packages. virtual private networking and the virtual private network (VPN) technologies supported by Windows Server 2003 and Windows XP and describes the set of features that provides advanced security capabilities and simplified administration of VPN connections for enterprise networks. Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol with Internet Protocol security (L2TP/IPSec) are described as the two industry standard methods for VPN connections. Intrusion detection system evasion techniques bypass detection by creating different states on the IDS and on the targeted computer. The adversary accomplishes this by manipulating either the attack itself or the network traffic that contains the attack.

IPsec is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3. Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell(SSH), operate in the upper layers of these models.

REFERENCES

1. Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.
2. Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International
3. Jackson, Kathleen, DuBois, David H., and Stallings, Cathy A., "A Phased Approach to Network Intrusion Detection," 14th National Computing Security Conference, 1991
4. D. Harkins and D. Carrel (Cisco Systems). "RFC 2409 The Internet Key Exchange (IKE)". Internet Engineering Task Force (IETF).
5. D. Xin, J. Han, X. Yan, and H. Cheng, "Mining Compressed Frequent-Pattern Sets," in Proceedings of the 31st international conference on Very Large Data Bases, pp. 709-720, 2005.
6. Artificial Intelligence (AAAI-98), RICH, C. and MOSTOW, J., Eds. AAAI Press, Menlo Park, CA. 46-53.